



X Family of Security Devices Hardware Installation Guide

Version 2.5.1

- X5
- X506

Part Number TECHD-220 Rev A01
Published April 2007

<http://www.3com.com/>



3Com Corporation
350 Campus Drive
Marlborough, MA
01752-3064

Copyright © 2006–2007, 3Com Corporation. All rights reserved. No part of this documentation may be reproduced in any form or by any means or used to make any derivative work (such as translation, transformation, or adaptation) without written permission from 3Com Corporation.

3Com Corporation reserves the right to revise this documentation and to make changes in content from time to time without obligation on the part of 3Com Corporation to provide notification of such revision or change.

3Com Corporation provides this documentation without warranty, term, or condition of any kind, either implied or expressed, including, but not limited to, the implied warranties, terms, or conditions of merchantability, satisfactory quality, and fitness for a particular purpose. 3Com may make improvements or changes in the product(s) and/or the program(s) described in this documentation at any time.

If there is any software on removable media described in this documentation, it is furnished under a license agreement included with the product as a separate document, in the hardcopy documentation, or on the removable media in a directory file named LICENSE.TXT or !LICENSE.TXT. If you are unable to locate a copy, please contact 3Com and a copy will be provided to you.

UNITED STATES GOVERNMENT LEGENDS:

If you are a United States government agency, then this documentation and the software described herein are provided to you subject to the following:

United States Government Legend: All technical data and computer software is commercial in nature and developed solely at private expense. Software is delivered as Commercial Computer Software as defined in DFARS 252.227-7014 (June 1995) or as a commercial item as defined in FAR 2.101(a) and as such is provided with only such rights as are provided in 3Com's standard commercial license for the Software. Technical data is provided with limited rights only as provided in DFAR 252.227-7015 (Nov 1995) or FAR 52.227-14 (June 1987), whichever is applicable. You agree not to remove or deface any portion of any legend provided on any licensed program or documentation contained in, or delivered to you in conjunction with guide.

Unless otherwise indicated, 3Com registered trademarks are registered in the United States and may or may not be registered in other countries.

3Com and the 3Com logo are registered trademarks of 3Com Corporation. TippingPoint, the TippingPoint logo, and Digital Vaccine are trademarks of 3Com Corporation or one of its subsidiaries.

Microsoft and Windows are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. Oracle is a registered trademark of Oracle Corporation.

Other brand and product names may be registered trademarks or trademarks of their respective holders.

Contents

About This Guide	5
Overview	5
Target Audience	5
Organization	6
Conventions	7
Headings	7
Typeface	7
Cross-References	7
Messages	7
Warning	7
Caution	8
Note	8
Tip	8
Related Documentation	9
Customer Support	9
Contact Information	9
 Chapter 1. Prepare the Site	 11
Overview	11
Safety Requirements	12
Class A Notices	12
Class B Notices	12
General Guidelines	13
Environmental Requirements	15
System Grounding Requirements	15
Unpack the System	16
 Chapter 2. Overview	 17
Overview	17
X Family Overview	17
Core Functionality	18
X Family Environment	18
Optimized VPN Connectivity	19
Policy Enforcement	19
Security Zones and Network Interfaces	19
IPS	20
Threat Suppression Engine	20
Local Security Manager	21
Security Management System	21
Threat Management Center	21

Chapter 3. 3Com X5 Overview 23

Overview	23
Chassis Overview	24
LEDs	24
Technical Specifications	25
Hardware Specifications	25
Technical Specifications	26
Software Specifications	26
Hardware Installation and Configuration	27
Determine Installation Location	27
Connect the Power	27
Complete Initial Setup Configuration	27
Connect the X5 to the Internet	28
Register the X5 Device	28
Troubleshooting the X5 Device	29
Cannot Access Device Through LAN Port	29

Chapter 4. 3Com X506 Overview 31

Overview	31
Chassis Overview	32
Chassis Features	32
LEDs	32
Technical Specifications	33
Hardware Specifications	33
Technical Specifications	34
Software Specifications	34
Hardware Installation and Configuration	35
Install the X506 Chassis	35
Determine Total Rack Space	35
Bolt the Device to the Rack	35
Connect the Power	36
Complete Initial Setup Configuration	36
Connect the X506 Device to the Internet	37
Register the 3Com X506 Device	37
Troubleshooting the X506 Device	37
Cannot Access Device Through LAN Port	38

Appendix A. Connector and Pinout Specifications 39

Port Connectors	39
X5 and X506 Port Connectors	39
Additional X506 Connectors	40

About This Guide

Explains who this book is intended for, how the information is organized, where information updates can be found, and how to obtain customer support if you cannot resolve a problem.

Overview

Welcome to the *X Family of Security Devices Hardware Installation Guide*. The 3Com X Family of security devices combines firewall and VPN functionality with the Intrusion Prevention System (IPS) to provide a unified approach to network security. The Local Security Manager (LSM) and Security Management System (SMS) provide management options for your X Family devices and network security.

This chapter includes the following sections:

- [“Target Audience” on page 5](#)
- [“Organization” on page 6](#)
- [“Conventions” on page 7](#)
- [“Related Documentation” on page 9](#)
- [“Customer Support” on page 9](#)

Target Audience

This guide is intended for use by technicians and maintenance personnel responsible for installing, configuring, and maintaining the X Family devices. Users should be familiar with telecommunications products and networking concepts.

Organization

The *X Family of Security Devices Hardware Installation Guide* is organized as follows:

- **About the Guide** — Explains who this book is intended for, how the information is organized, where information updates can be found, and how to obtain customer support if you cannot resolve a problem.
- **X Family Overview** — Provides a description of the deployment environment of the X Family devices, including layout and illustrations of hardware components and features.
- **Prepare the Site** — Provides general requirements for the installation site and guidelines for electrical and network connections. For specific requirements, review the chapter according to device model.
- **X5 Overview** — Provides a description of the deployment environment of the X5 device, including layout and illustrations of hardware components and features.
- **X506 Overview** — Provides a description of the deployment environment of the X506, including layout and illustrations of hardware components and features.
- **Appendix A: Connector and Pinout Specifications** — Provides connector and pinout information for the X Family devices.

Conventions

This book and the other books in this series follow conventions for structuring information as described next.

Headings

Every chapter starts with a brief description of the information that you can find in that chapter, which correlates with the major headings in that chapter. Each major heading corresponds to a task or concept that is important for you to understand. Headings are of a different size and type to make them easy to skim, whether you are viewing an online or print copy of this document.

Typeface

This book uses the following typeface conventions:

Bold	Used for the names of screen elements like buttons, drop-down lists, or fields. For example, when you are finished with a dialog box, you click the OK button.
<code>Code</code>	Used for text that the user must type to use the product.
<i>Italic</i>	Used for book titles, variables, and important terms.
Hyperlink	Used for web site and cross-reference links.

Cross-References

When a topic is covered in depth elsewhere in this guide or in another book in this series, a cross-reference to the other information will be provided. Cross-references within this book take this form: “For more information about conventions, see page 6, Conventions.” Cross-references to other publications take this form: “For more information about <topic>, see *Publication Name*.”

Messages

Messages are special text that are emphasized by font, format, and icons. 3Com documents have four types of messages:

- Warning
- Caution
- Note
- Tip

A description of each message type with an example message follows.

Warning

Warnings tell you how to avoid physical injury to people or equipment. For people, injury includes anything from temporary conditions, such as pain, to irreversible conditions such as death. For equipment, injury means anything requiring repair. Warnings tell you what you should or should not do, and the consequences of not heeding the warning.

Warnings have an icon to the left showing a white lightning bolt drawn inside of a red octagon. Warnings also start with the word “WARNING” and are presented in boldface type.



WARNING: Only trained and qualified personnel should install, replace, or service this equipment. Disconnect the system before servicing.

Caution

Cautions tell you how to avoid a serious loss that stops short of physical damage such as the loss of data, time, or security. Cautions tell you what you should or should not do to avoid such losses, and the consequences of not heeding the caution.

Cautions have an icon to the left showing a black exclamation point drawn inside of a yellow triangle. Cautions also start with the word “CAUTION”.



CAUTION: Do not type `del *.*` from the root (C:\) directory. Typing `del *.*` from the root directory will destroy all the program and configuration data that your computer needs to run, and will render your system inoperable.

Note

Notes tell you about information that might not be obvious, or that does not relate directly to the current topic, but that may affect relevant behavior.

A note has an icon to the left showing a piece of note paper, and starts with the word “Note”.



Note: Most car rental companies no longer allow cash deposits in lieu of a credit card when renting a car. Non-credit card deposits can only be arranged by a lengthy application and approval process.

Tip

Tips are suggestions about how you can perform a task more easily or more efficiently.

A tip has an icon to the left showing a light bulb drawn inside and starts with the word “Tip.”



Tip: Setting the **logging** parameter to “off” or “minimal” will improve your system’s processing performance, but it will make debugging very difficult in the event of a system crash. During system integration, you can set logging to “full” to ease debugging. After you have finished testing, set logging to “minimal” to improve performance.

Related Documentation

The X Family devices have a full set of documentation. These publications are available in electronic format on your Documentation CDs. For the most recent updates and for Release Notes, visit

www.3com.com

Customer Support

3Com is committed to providing high-quality customer support to all of its customers. A customer is provided with detailed customer and support contact information. For the most efficient resolution of your problem, please take a moment to gather some basic information from your records and from your system before you contact 3Com customer support.

Information	Location
Your X Family serial number	You can find this number in the LSM in the <i>System Summary</i> page, on the shipping invoice that came with your X Family system, or on the bottom of the device.
Your TOS version number	You can find this information in the LSM in the <i>System Summary</i> page, or by using the CLI <code>show version</code> command.
Your X Family device system boot time	You can find this information in the LSM in the <i>System Summary</i> page.

Contact Information

Please address all questions regarding the 3Com software to your authorized 3Com representative. For customer support contact information, refer to the release notes that ship with your device.

1 Prepare the Site

This chapter discusses the general requirements necessary to prepare your site for the installation of the 3Com X Family device.

Overview

Before you install your new 3Com X Family security device, you need to gather materials and prepare the network and hardware site. To carefully and correctly install the components, you must read through all preparation instructions and requirements. This chapter includes general guideline information for all devices in the family.

This chapter covers these topics:

- [“Safety Requirements” on page 12](#)
- [“Environmental Requirements” on page 15](#)
- [“System Grounding Requirements” on page 15](#)
- [“Unpack the System” on page 16](#)

Safety Requirements

If not properly installed and maintained, electrical circuitry equipment like the 3Com X Family devices can pose dangers to both personnel and equipment. To prevent accidents, adhere to the following guidelines to ensure general safety:

- Remove any dust from the area and keep the area around the 3Com X Family system clear and dust-free during and after installation.
- Wear safety glasses if you are working under conditions that might be hazardous to your eyes.
- There are no serviceable parts inside the chassis.

Class A Notices

The X506 is a Class A device. Read and follow all of the notices and safety instructions in the document called *3Com Hardware Compliance X Family Class A Notice*, which is shipped in the box with the X506.

Class B Notices

The X5 is a Class B device. Read and follow all of the notices and safety instructions in the document called *Regulatory Information for the 3Com X5 Security Device*, which is shipped in the box with the X5.

General Guidelines

Read and follow these cautions and warnings for further safety guidelines.

CAUTION: Before you start the installation procedures, read this entire chapter for important information and safety warnings.

Use proper electrostatic discharge (ESD) protection when you handle equipment.

Do not power up the equipment while you install and connect the system.



For rack-mountable equipment, the equipment rack must be anchored to an unmovable support to prevent it from falling over when one or more servers are extended in front of it on slide assemblies. The equipment rack must be installed according to the manufacturer's instructions. You must also consider the weight of any other device installed in the rack.

For rack-mountable equipment, you are responsible for installing an AC power disconnect for the entire rack unit. This main disconnect must be readily accessible, and it must be labeled as controlling power to the entire unit, not just to the server.

Make sure that the chassis cooling fans run continuously while the system is powered.

Use of controls or adjustments or performance of procedures other than those specified herein may result in hazardous radiation exposure.



WARNING: Only trained and qualified personnel should install, replace, or service this equipment. Disconnect the system before servicing it. There are no user-replaceable parts in the chassis.

This product requires short-circuit (overcurrent) protection to be provided as part of the building installation. Install only in accordance with national and local wiring regulations.

Do not operate the system unless top cover is in place.

To reduce the risk of fire, use only No. 26 AWG or larger telecommunication line cord.

The battery in this unit is not replaceable. There is a risk of explosion if the battery is replaced by an incorrect type. Dispose of used batteries according to the instructions.

This equipment is to be installed and maintained by service personnel only as defined by AS/NZS 3260 Clause 1.2.14.3 Service Personnel.

This unit is intended for installation in restricted access areas only.

When connecting equipment to IT power distributions, Phase to phase voltage must not exceed 240 V.

The ports on the front of the 3Com X Family devices are Safety Extra-Low Voltage (SELV) circuits. SELV circuits should only be connected to other SELV circuits.

Do not work on the system or connect or disconnect cables during periods of lightning activity.

To prevent the unit from overheating, do not operate it in an area that exceeds the maximum recommended ambient temperature of 104° F (40° C). To prevent airflow restriction, allow at least 3 inches (7.6 cm) of clearance around the ventilation openings.



WARNING: Read all of the installation instructions before you connect the system to its power source.

Never touch uninsulated telephone wires or terminals unless the telephone line has been disconnected at the network interface.

Do not operate the system unless all faceplates and covers are in place. Faceplates and cover panels serve three important functions: They prevent exposure to hazardous voltages and currents inside the chassis; they contain electromagnetic interference (EMI) that could disrupt other equipment; and they direct the flow of cooling air through the chassis.

To prevent personal injury or damage to the chassis, lift the chassis from beneath its lower edge.

For rack-mountable equipment, enclosed racks may have higher ambient temperatures than open racks. Ensure that enclosed racks' ambient temperatures do not exceed maximum recommended ambient temperature of 104 °F (40 °C).

Environmental Requirements

In order for the 3Com X Family device to run properly, your environment must meet the proper criteria.

The following table lists the recommendations for temperature, humidity, and altitude settings for the Service Provider (SP) environment.

Table 1 - 1: Environmental Requirements for the 3Com X Family

Environmental Specifications	Description
Temperature	0 to 40 °C (32 to 104 °F) — Operating -20 to 80° C (-4 to 176 ° F) — Storage
Humidity	5 to 95% (non-condensing)
Altitude	No degradation up to 13K feet above sea level

System Grounding Requirements

Damage from electrostatic discharge (ESD) can occur when electronic components are improperly handled. This damage can result in complete or intermittent system failures. Proper ESD protection is required whenever you handle equipment. It is not necessary to open the chassis to add or remove any components. The unit has no replaceable parts inside it.

Unpack the System

Each system chassis is securely packaged in a shipping box.



CAUTION: ESD can damage the 3Com X Family device if you do not take necessary precautions. Installation and maintenance personnel should be properly grounded using ground straps to eliminate the risk of ESD damage to the equipment.

Use caution when opening the 3Com X Family boxes.

To unpack the 3Com X Family device

- STEP 1** Inspect the packing container. If you see any damage or other signs of mishandling, inform both the local freight provider and 3Com before you unpack the device. Your freight provider can provide you with the procedures necessary to file a claim for damages.
- STEP 2** Carefully open the box.
- STEP 3** Remove all packing material.
- STEP 4** Verify the contents in the shipping package. Compare the packing list to your shipment and to your order. If items are missing, contact your sales or field representative.
- STEP 5** Remove the chassis from the box.
- STEP 6** Open the accessory kit. It contains the cables, documentation, and Documentation CD.
- STEP 7** Inspect all the equipment inside for damage. If you think any equipment might be damaged, contact your freight provider for how to lodge a damage claim and contact your sales or field representative for instructions.



Please Recycle: The shipping materials are recyclable. Please save them for later use or dispose of them appropriately.

2 Overview

This chapter introduces system concepts and functionality. It provides an overview of the X Family.

Overview

In the highly technical era of data transfers and the Internet, the protection of data and networks concerns most businesses, corporations, and network administrators. 3Com has studied the issue of data security and network protection from malicious activity and attacks. One of the solutions is the X Family of security devices (X Family). The X Family devices provide constant vigilance for a network by monitoring and managing packets while blocking malicious attacks.

This chapter covers these topics:

- [“X Family Overview” on page 17](#)
- [“X Family Environment” on page 18](#)

X Family Overview

The X Family of security devices combines virtual private network (VPN) management, stateful packet inspection firewall, bandwidth management, and web content filtering with the Intrusion Prevention System (IPS).

The IPS provides total packet inspection and intrusion prevention. The IPS detects and blocks inappropriate, incorrect, or anomalous activity on the network by comparing network traffic with *filters* defined by the 3Com TippingPoint Division. The X Family devices use filters to scan traffic and recognize header or data content in the attack along with the protocol, service, and the operating system or software that the attack affects. The attack filter includes an *action set*, which defines the reaction when the X Family device encounters packets that match attack filter parameters. In a broad sense, the X Family device either drops matching packets or permits them.

The Stateful firewall provides service-level, stateful inspection of network traffic before it is inspected by the IPS. It incorporates filtering functionality to protect mission-critical applications. An

administrator can use firewalls and content filters that determine how the system handles traffic to and from a particular service. These filters are specified by the source, destination, and service or protocol of the traffic. Network Address Translation (NAT) provides the capability to share a single IP address, or to define Virtual Servers for public services such as web sites.

Core Functionality

The X Family device provides the following core functionality:

- Optimized VPN connectivity — The device allows inspection and control of traffic both inside and outside of VPN tunnels.
- Enforcement of usage policies — The device can be used to rate-limit applications, such as peer-to-peer file sharing applications. It includes an optional Web Content Filter subscription service. for preventing access to undesirable Web sites.
- Multicast applications — The device prioritizes real-time traffic and provides secure connectivity for IP multicast traffic.
- Detection and suppression — Unlike an intrusion detection system (IDS), the device identifies and *stops* malicious traffic on the edge of the network.
- Filter customization — Through IP filters, exceptions, and attack filter creation, you can customize the system to meet the specific needs of your enterprise.
- Real-time threat aggregation — The TMC collects threat information from throughout the world, converts it to attack filters, and distributes it to customers.
- Monitoring — The integrated reports generated by the device show graphically what traffic is going through the device to what servers. This includes visibility on web site access and type of traffic being transferred.
- Dynamic routing — The device can participate in dynamic routing via RIPv1/RIPv2 or static routes.
- Central management and reporting via the TippingPoint Security Management System (SMS) — available separately. SMS allows bulk configuration of all features of the device, including easy creation of VPN tunnels. SMS also offers centralized report generation and log collation.

The following sections describe each security application in more detail.

X Family Environment

A single X Family device can be installed at the perimeter of your network, on your Intranet, or both.

All of the functionality of the devices runs directly on the device as the Operating System (TOS). The Local Security Manager (LSM) is a web-browser client for managing your device that provides a graphical interface for on-the-box administration, configuration, and reporting. The LSM accesses the functionality of the X Family TOS.

You can also access the functionality of the device using the Command Line Interface (CLI). The CLI provides a way for you to set values, run setup commands, and perform general functions. However, the LSM provides most of the same functionality, except for some advanced configuration commands. In addition the LSM provides reporting and filter configuration.

The Security Management System (SMS) provides functionality beyond that provided by the LSM and CLI. The SMS enables you to manage not one but multiple devices. The SMS coordinates all X Family and IPS devices across your environment for administration, configuration, and monitoring. Most important, the SMS includes enterprise-wide reporting and trend analysis.

From the SMS, you must set an overall profile of settings for each X Family device. The profile controls how the device responds to traffic that matches filters. The X Family device is always in *Active* mode and reacts to traffic as specified by the appropriate filter.

The LSM and the X Family device maintain a connection to the Threat Management Center (TMC), which is located at TippingPoint headquarters. The TMC monitors 10,000 sensors around the world for the latest attack information. As a result, your network can be continually inoculated.

Each component of the X Family environment is discussed in more detail in the following sections. Additional information about the X Family devices is available in the *X Family Concepts Guide*.

Optimized VPN Connectivity

The X Family VPN features support IPSec, L2TP, and PPTP tunneling protocols, as well as DES, 3DES, AES-128/192/256, MD5, and SHA-1 encryption standards, and manual keyring, IKE with pre-shared keys, and IKE with X.509 certificates. The device provides intrusion prevention inspection within VPN tunnels and can also prioritize traffic bi-directionally, both inside and outside of the VPN tunnels. The VPN is hardware-accelerated, with an ASIC designed specifically for encrypting and decrypting packets. To increase network security, you can configure VPN traffic to terminate in a security zone that is separate from your internal LAN security zones. The X Family devices also support NAT deployment within VPN tunnels.

Policy Enforcement

Policy enforcement includes the X Family device firewall, content filtering, and the IPS. The X Family device has a stateful inspection firewall with a top-down rule evaluation engine. The firewall can be used to rate-limit both security zones and applications, preventing excess bandwidth consumption. 3Com offers a Web Filtering subscription service, which allows or denies web sites by category. You can also manually allow or block URLs as exceptions to the defined rules. Web Filtering is applied through firewall rules.

Security Zones and Network Interfaces

Security Zones enable you to segment your network into trusted areas. Traffic within a security zone is switched at wire speed and is not inspected. Traffic between two security zones is inspected by the firewall, IPS, and other security services. A security zone can be associated with one or more physical ports or can exist only virtually by logical definition (no ports). A virtual zone is useful for terminating VPNs such that traffic can be inspected within the VPN tunnel after decryption as part of routing to the destination security zone. Policy enforcement is applied to traffic that moves between security zones. Network virtual interfaces enable you to connect multiple Layer 3 networks to the X family device. Each Security Zone needs to be associated with a Virtual Interface. A Virtual Interface can be associated with multiple security zones in a transparent/bridged deployment where security is still enforced but the device is deployed easily into an existing Layer 2 network. Security zones can be defined through 802.1q VLAN tags.

IPS

X Family devices use the IPS to protect your network by scanning, detecting, and responding to network traffic according to the filters, action sets, and global settings maintained on each device by a client. Each device provides intrusion prevention for your network according to the amount of network connections and hardware capabilities.

The IPS is designed to handle the extremely high security demands of carriers and high-density data centers. This functionality has been scaled down into the X Family, providing unprecedented attack prevention for smaller deployments. Even while under attack, Intrusion Prevention Systems are extremely low-latency network infrastructure ensuring switch-like network performance.

The IPS is an active network defense component that uses the Threat Suppression Engine (TSE) to detect and respond to attacks. Intrusion Prevention Systems are optimized to provide high-resiliency, high-availability security for remote branch offices, small-to-medium and large enterprises, and collocation facilities. Each system can protect network segments from both external and internal attacks.

X Family devices provide the following Ethernet interfaces and traffic performance:

Table 2 - 1: X Family System Performance

Model	Ethernet interfaces	Concurrent sessions	IPS Performance	Firewall Performance	Triple DES
X5, 25-user license	6 x 10/100	20,000	18 Mbps	50 Mbps	40 Mbps
X5, unlimited-user license	6 x 10/100	60,000	18 Mbps	50 Mbps	40 Mbps
X506	6 x 10/100	128,000	50 Mbps	100 Mbps	95 Mbps

Threat Suppression Engine

The Threat Suppression Engine (TSE) is a highly specialized, hardware-based intrusion prevention platform. The TSE is a high-performance software engine that contains all the functions needed for Intrusion Prevention, including IP defragmentation, TCP flow reassembly, statistical analysis, traffic shaping, flow blocking, flow state tracking, and application-layer parsing of over 170 network protocols.

The TSE reconstructs and inspects flow payloads by parsing the traffic at the application layer. As each new packet of the traffic flow arrives, the engine reevaluates the traffic for malicious content. The instant the engine detects malicious traffic, it blocks all current and all subsequent packets pertaining to the traffic flow. The block of the traffic and packets ensures that the attack never reaches its destination.

The highly specialized traffic classification engines enable the IPS to filter with extreme accuracy.

Local Security Manager

The Local Security Manager (LSM) is responsible for local administration, configuration, and reporting for a single X Family device. Through a graphical user interface (GUI), the LSM provides the interfaces, tools, and processes that configure and monitor the X Family device. The LSM provides a subset of the management functionality offered through the Security Management System, which is designed to manage several X Family units from a central server.

You access the LSM through a web browser (Internet Explorer V6 or Firefox). The application accesses the Operating System and settings stored on the device. Through the LSM, you can manage settings directly to the device. You access each device to use the LSM. The LSM is not a central application that accesses each device in turn. Rather, it resides as a graphical client for managing the device.

For more detailed information, see the *Local Security Manager User's Guide*.

Security Management System

The Security Management System (SMS) provides a global view and control for the X Family environment. It is shipped as a management server and includes an enterprise desktop — the workstation client — through which end users can perform secure, policy-based management tasks for multiple X Family devices. It provides facilities similar to the LSM but supports a larger scope. Most important, it provides enterprise-wide reporting.

Unlike the LSM, the SMS client provides a central application for managing multiple X Family devices. You can create multiple profiles of firewall rules, IPS filters, VPNs, and more to distribute to specific devices organized in segment groups. You can also update the TOS software updates, Digital Vaccine packages, and configuration settings for all devices through the SMS.

For more detailed information, see the *TippingPoint Security Management System User's Guide* on the Documentation CD that is shipped with your X Family device.

Threat Management Center

The Threat Management Center (TMC) is the central intelligence bureau for the X Family environment. The TMC performs comprehensive global reconnaissance for emerging threats. It rapidly builds new filters and algorithms to suppress such threats.

The TMC offers the following end-user services:

- Digital Vaccine — A subscription service that offers real-time continuous update capability. With Digital Vaccine, the X Family devices pull new threat filters from the TMC on a routine basis.
- Software Updates — Upgraded and updated versions of the software that you can use for your X Family device, including the Local Security Manager and Security Management System
- Technical Support — Information on how to contact 3Com and receive technical support for user issues

3 3Com X5 Overview

This chapter provides an overview of the X5 device.

Overview

This chapter describes the components, chassis, requirements, and installation of the X5 device.

Before you install the X5 device, read the *Quick Start Guide for the X5* (which is shipped in the box with the unit) and download the *X Family Command Line Interface Reference* from the Documentation CD that is shipped with the unit. After you install the components, you must run the Setup Wizard as part of the installation and configuration procedures.

This chapter includes the following topics:

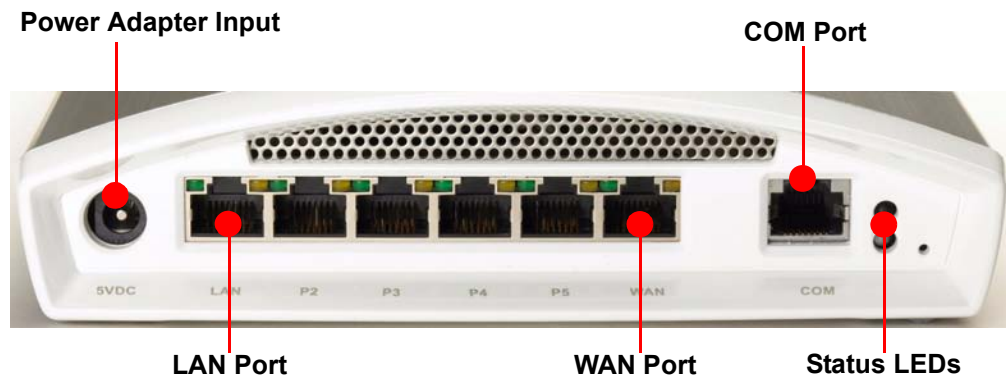
- [“Chassis Overview” on page 24](#)
- [“Technical Specifications” on page 25](#)
- [“Hardware Installation and Configuration” on page 27](#)

Chassis Overview

The X5 comprises a compact chassis that does not require installation on a server rack. The X5 uses a front-access, 6-port architecture, supporting connections to up to 16 network security zones.

The following image shows the front chassis interface for the X5 device.

Figure 3 - 1: X5 - Front Panel



LEDs

The following table describes the Status LEDs.

Table 3 - 1: Status LED Descriptions

LED	Color	State	Description
Top LED	Flashing	Booting	Indicates that the X5 is booting up
	Solid green	Operational	Indicates that the X5 is online
Bottom LED	Flashing	Establishing VPN	Indicates that the VPN connection is in the process of being established
	Solid green	Operational	Indicates that all configured VPN connections are established successfully
	Solid green, slow flash	Established with traffic	Indicates that the established VPN connections are passing data traffic

The following table describes the Link and Activity LEDs that are at the upper left and right corners of each Ethernet port.

Table 3 - 2: Ethernet Port LED Descriptions

LED	Color	State	Description
Activity LED	No light	No traffic	Indicates that the port is not ready and is not passing traffic, or is malfunctioning
	Blinking amber	Operational	Indicates that the port is passing data
Link	No light	No traffic	Indicates that the link is not active
	Green	Operational	Indicates that the link is active

Technical Specifications

The following sections describe the hardware, technical, and software specifications for the X5.

- [“Hardware Specifications” on page 25](#)
- [“Technical Specifications” on page 26](#)
- [“Software Specifications” on page 26](#)

Hardware Specifications

The following table lists hardware specifications for the X5.

Table 3 - 3: X5 Specifications

Specification	Description
Dimensions	11.5 in. x 6.6 in. x 1.8 in (29 cm x 17 cm x 4 cm)
Weight	3.25 lb (1.21 kg)
Serial Interface	RJ45 interface: COM1; 115200 baud; parity: none
Network Interfaces	6 copper ports
Power Requirements	100 to 240 VAC; 0.8-0.4 amperes @ 50-60 Hz; maximum power consumption: 30 Watts

Table 3 - 3: X5 Specifications

Specification		Description
Service Provider operating requirements	Temperature	Operating: 0 to 40 ° C (32 to 104 ° F) Storage: –20 to 70° C (–4 to 158° F)
	Altitude	No degradation up to 13K feet
	Humidity	5% to 95% (noncondensing)



Note: Use only the supplied wall-mounted power supply. Do not use other power supplies with the X5 device.

Technical Specifications

The following table lists technical specifications.

Table 3 - 4: X5 Hardware Specifications

Specification	Detail	Description
Power consumption		Max 30W
External interfaces		Six 10/100 Ethernet one RJ45 serial

Software Specifications

To configure the X5 device you need one of the following software applications or devices.

Table 3 - 5: Configuration Requirements for the X5 Device

Specification	Description
X Family Security Management System (SMS) Software, Version 2.5 and above. (optional)	SMS can optionally be used to manage multiple Intrusion Prevention Systems.
1 Windows-based PC running Windows 9x, NT, 2000, XP, or ME	Must be attached to your network via PC serial port.

Hardware Installation and Configuration

This section includes the following topics:

- [“Determine Installation Location” on page 27](#)
- [“Connect the Power” on page 27](#)
- [“Complete Initial Setup Configuration” on page 27](#)
- [“Connect the X5 to the Internet” on page 28](#)
- [“Register the X5 Device” on page 28](#)

Determine Installation Location

The X5 is a compact device that does not require rack installation. Place it in a location with adequate ventilation. Do not block or cover it with any other devices or objects.

Connect the Power

The X5 includes a 5V DC power supply. Use only the supplied power supply. Do not use other power supplies with the X5 device.

STEP 1 Plug the power supply into the input connector on the front of the X5 device.

STEP 2 Plug the power supply into an AC outlet, power strip, or UPS.



CAUTION: The X5 device may take several minutes to boot up. When the Status LED is steady green, the device is powered up and ready to use.

Complete Initial Setup Configuration

STEP 1 Configure your computer's network connection to receive an IP address by DHCP.

STEP 2 Use an Ethernet cable to connect your computer directly to the X5 LAN port. Your computer will receive an IP address from the X5 device.

STEP 3 In your PC's internet browser, connect to the X5 default LAN address (<https://192.168.1.254>).

STEP 4 The OBE wizard opens. Take these steps:

STEP A Accept the default security level of Level 2.

STEP B Specify the SuperUser account information at the prompt:

- User Name
- Password
- Confirm password

STEP C Accept the default settings in the rest of the Setup Wizard: Select **No** at the prompt.

STEP D Depending on your internet connectivity, you may need to update your WAN settings in the Virtual Interfaces setup screen.

- If you use DHCP to connect to your Internet provider, accept the default WAN settings.
- If you use PPPoE, enter your ISP user name and password.
- If your ISP assigns a static IP address, select **Static** as the external interface type and enter the IP address, subnet mask, and default gateway information.

STEP E Define additional user accounts if desired.

At this point, your initial configuration of the X5 is complete. You can now use the LSM to change settings in the future.



Note: When you connect to the LAN address, your browser may display a security certificate warning. Accept the certificate and continue with the configuration procedure.

Connect the X5 to the Internet

- STEP 1** Use an Ethernet cable to connect the X5 WAN port to your router. If the X5 is configured to receive its WAN IP address by DHCP, PPPoE, PPTP, or L2TP, the device connects to your service provider. This may take a minute or more.
- STEP 2** Check the status of the external virtual interface with the LSM or the CLI. If active, the interface will be in “Up” status and will have an IP address.
- STEP 3** Use your web browser to connect to an external URL, such as <http://www.3com.com>. If you can see the web site, your internet connection is active, and you can register your device and configure other features of the X5.

Register the X5 Device

To activate your license, you must register the X5 device on the 3Com eSupport Web site (<http://esupport.3com.com>). Have the following information available:

- Product code.
 - 3CRTPX5-U-96 for unlimited user licenses.
 - 3CRTPX5-25-96 for 25-user licenses.
- Serial number. You can find the serial number:
 - in the Local Security Manager (LSM), on the **System Summary** page.
 - with the Command Line Interface (CLI) `show version` command.
 - on the bottom of the X5 unit, on the bar code sticker.
- Product purchase information:
 - Company Purchased From
 - Purchase Location City
 - Warranty Start Date, in the format *mm/dd/yyyy*
- Digital Vaccine license key.

Troubleshooting the X5 Device

This section describes procedures for troubleshooting your X5 device.

Cannot Access Device Through LAN Port

- STEP 1** Check the LAN port LEDs. If the green Link LED is off, the port is not active. Check that you are connected to port 1 (LAN) on the device.
- STEP 2** Check that your PC has received an IP address from the device. This will be in the range 192.168.1.1 to 192.168.1.20. If not, check that your PC is configured for DHCP IP address allocation.
- STEP 3** Try to ping the device from the PC at address 192.168.1.254. If the device responds, then it is booted and running.

If none of the above steps help, then contact 3Com Technical Support.

4 3Com X506 Overview

This chapter provides an overview of the 3Com X506 security device.

Overview

This chapter describes the components, chassis, requirements, and installation of the 3Com X506 security device.

Prior to installation, you should also obtain the *3Com X Family Command Line Interface Reference*. After you install components, you must run through the Setup Wizard as part of the installation and configuration procedures.

This chapter includes the following topics:

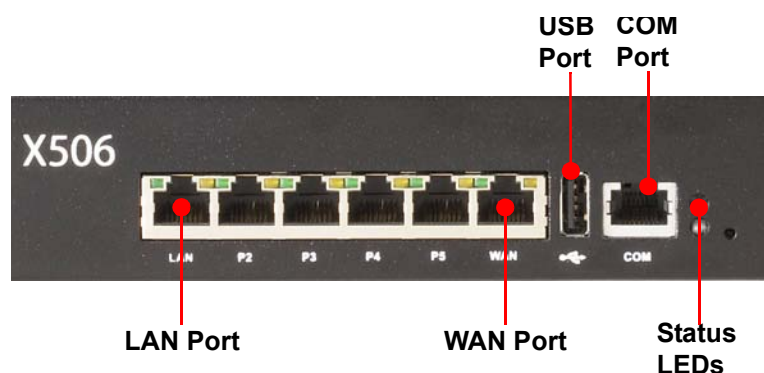
- [“Chassis Overview” on page 32](#)
- [“Technical Specifications” on page 33](#)
- [“Hardware Installation and Configuration” on page 35](#)

Chassis Overview

The 3Com X506 system comprises a 1-rack-unit chassis with a front-access architecture. The X506 has 6 ports, supporting up to 6 network segments. It is rack-mountable on a 19- or 23-inch rack.

The following image shows the front chassis interface for a X506.

Figure 4 - 1: 3Com X506 - Front Panel



The following sections describe the X506 hardware components.

Chassis Features

The chassis offers features for viewing the status of the system and modifying settings.

LEDs

The two status LEDs on the front panel are described in the following table.

Table 4 - 1: X506 LED Descriptions

LED	Color	State	Description
Top LED	Flashing green	Bootup	Indicates that the system is booting up.
	Solid green	Operational	Indicates that the system is powered and operating properly.
Bottom LED	Flashing	Establishing VPN	Indicates that the VPN connection is in the process of being established.
	Solid green	Operational	Indicates that all configured VPN connections are established successfully.
	Solid green, slow flash	Established with traffic	Indicates that the established VPN connections are passing data traffic.

The following table describes the Link and Activity LEDs that are at the upper left and right corners of each Ethernet port.

Table 4 - 2: Segment Port LED Descriptions

LED	Color	State	Description
Link (left side LED)	No light	No link	Indicates that the port is not linked.
	Green	Active	Indicates that the port is connected and ready for data.
Activity (right side LED)	No light	No traffic	Indicates that the port is not passing data.
	Blinking amber	Data Traffic	Indicates that port is passing data.

Technical Specifications

The following sections list the hardware, technical, and software specifications for the 3Com X506.

- [“Hardware Specifications” on page 33](#)
- [“Technical Specifications” on page 34](#)
- [“Software Specifications” on page 34](#)

Hardware Specifications

The following table lists hardware specifications for the X Family X506.

Table 4 - 3: X Family X506 Specifications

Specification	Description
Dimensions	17.25 in. x 12.25 in. x 1.75 in. (43.8 cm x 31.1 cm x 4.4 cm)
Weight	9 lbs (2.2 kg)
Serial Interface	RJ45 interface - COM1; 115200 baud; parity: none; flow control: none
Network Interfaces	Six 10/100 Ethernet copper interfaces.
Power Requirements	100 to 240 VAC; 1-2 amperes @ 50-60 Hz; Maximum Power Consumption: 64 Watts

Table 4 - 3: X Family X506 Specifications

Specification		Description
Service Provider operating requirements	Temperature	Operating: 0 to 40 ° C (32 to 104 ° F) Storage: –20 to 70° C (–4 to 158 ° F)
	Altitude	No degradation up to 13K feet
	Humidity	5% to 95% (noncondensing)

Technical Specifications

The following table lists technical specifications for the X506 hardware.

Table 4 - 4: 3Com X506 Hardware Specifications

Specification	Detail	Description
Power consumption		Max 64W
External interfaces		One 10/100 Ethernet, one USB port, 6 copper ports



WARNING: The X506 device uses double pole/neutral fusing. To protect against risk of fire, replace X506 fuses only with the same type of fuse (5x20mm, 2A, 250 volts, fast-acting). Disconnect the power source before replacing the fuses.

Software Specifications

To configure the X506 device, you need one of the following software applications or devices.

Table 4 - 5: Configuration Requirements for the X506 Device

Specification	Description
Security Management System (SMS) Software, Version 2.5 and above (optional)	SMS can optionally be used to manage multiple Intrusion Prevention Systems.
1 Windows-based PC running Windows 9x, NT, 2000, XP, or ME	Must be attached to your network via serial port

Hardware Installation and Configuration

This chapter covers the following topics:

- [“Install the X506 Chassis” on page 35](#)
- [“Connect the Power” on page 36](#)
- [“Complete Initial Setup Configuration” on page 36](#)
- [“Connect the X506 Device to the Internet” on page 37](#)
- [“Register the 3Com X506 Device” on page 37](#)

Install the X506 Chassis

To install the TippingPoint follow the steps in these sections:

- [Determine Total Rack Space](#)
- [Bolt the Device to the Rack](#)

Determine Total Rack Space

Before you install the chassis, you must determine the total rack space that is required. The required rack space increases if you plan to install multiple systems.

The X506 device fits in either a 19-inch or a 23-inch wide rack. See the following table for individual rack space requirements.

Table 4 - 6: Rack Space Requirements

Requirement	Configuration Type	Min/Max Number of Chassis
Physical Size of Rack: Total number of chassis < or = 42 RUs Each X506 requires 1RU	Typical	Maximum of 9 chassis on a 7-foot rack
Network Equipment Building Systems (NEBS): Total number of chassis must generate: < or = 1372 Watts	Typical	13 chassis generating < or = 105 Watts

Bolt the Device to the Rack

Use the following guidelines when you bolt the X506 to the rack:



WARNING: To prevent bodily injury when mounting or servicing this unit in a rack, you must take special precautions to ensure that the system remains stable.

- If the rack comes with stabilizing devices, install the stabilizers before you mount or service the unit in the rack.
- If the rack is partially filled, load the rack from the bottom to the top, with the heaviest component at the bottom of the rack.
- If you plan to expand your system to include additional X Family systems in the future, allow space in the rack for additions. During the initial installation, keep in mind the weight distribution and stability of the rack.

Connect the Power

- STEP 1** Locate the male power inlet on the back of the chassis.
- STEP 2** Plug one end of a standard female power plug into the power inlet
- STEP 3** Plug the other end into an AC outlet or power strip and press the power switch to power on.



CAUTION: The X506 may take several minutes to boot up. When the Status LED is steady green, the device is powered up and ready to use.

Complete Initial Setup Configuration

- STEP 1** Configure your computer's network connection to receive an IP address by DHCP.
- STEP 2** Use an Ethernet cable to connect your computer directly to the X506 LAN port. Your computer will receive an IP address from the X506 device.
- STEP 3** With your computer's internet browser, connect to the X506 default LAN address (<https://192.168.1.254>).
- STEP 4** The OBE wizard opens. Take these steps:
- STEP A** Accept the default security level of Level 2.
 - STEP B** Specify the SuperUser account information at the prompt:
 - User Name
 - Password
 - Confirm password
 - STEP C** Accept the default settings in the rest of the Setup Wizard by clicking **No** at the prompt.
 - STEP D** Depending on your internet connectivity, you may need to update your WAN settings in the Virtual Interfaces setup screen.
 - If you use DHCP to connect to your Internet provider, accept the default WAN settings.
 - If you use PPPoE, enter your ISP user name and password.
 - If your ISP assigns a static IP address, select **Static** as the external interface type and enter the IP address, subnet mask, and default gateway information.

STEP E Define additional user accounts if wanted.

At this point, your initial configuration of the X506 is complete. You can use the LSM to change settings in the future.



Note: When you connect to the LAN address, your browser may display a security certificate warning. Accept the certificate and continue with the configuration procedure.

Connect the X506 Device to the Internet

- STEP 1** Use an Ethernet cable to connect the X506 WAN port to your router. If the X506 is configured to receive its WAN IP address by DHCP, PPPoE, PPTP, or L2TP, the device connects to your service provider. This may take a minute or more.
- STEP 2** Check the status of the external virtual interface with the LSM or the CLI. If active, the interface will be in “Up” status, and will have an IP address.
- STEP 3** Use your web browser to connect to an external URL, such as <http://www.3com.com>. If you can see the web site, your internet connection is active, and you can register your device and configure other features of the X506.

Register the 3Com X506 Device

To activate your license, you must register the 3Com X506 device on the 3Com eSupport Web site (<http://esupport.3com.com>). Have the following information available:

- Product code 3CRX506.
- Serial number. You can find the serial number:
 - in the Local Security Manager (LSM), on the **System Summary** page.
 - with the Command Line Interface (CLI) `show version` command.
- Product purchase information:
 - Company Purchased From
 - Purchase Location City
 - Warranty Start Date in the format *mm/dd/yyyy*
- Digital Vaccine license key.

Troubleshooting the X506 Device

This section describes procedures for troubleshooting your X506 device.

Cannot Access Device Through LAN Port

- STEP 1** Check the LAN port LEDs. If the green Link LED is off, the port is not active. Check that you are connected to port 1 (LAN) on the device.
- STEP 2** Check that your PC has received an IP address from the device. This will be in the range 192.168.1.1 to 192.168.1.20. If not, check that your PC is configured for DHCP IP address allocation.
- STEP 3** Try to ping the device from the PC at address 192.168.1.254. If the device responds, then it is booted and running.

If none of the above steps help, then contact 3Com Technical Support.

A

Connector and Pinout Specifications

This appendix provides connector and pinout information for the X5 and X506 systems.

Port Connectors

X5 and X506 Port Connectors

The X5 and X506 support 10/100 RJ-45 connectors, which have pinouts as described in this section.

The following figure displays an RJ-45 connector.

Figure A - 1: RJ-45 Connector



The following table describes the pinout information for a 10/100 RJ-45 connector.

Table A - 1: RJ-45 10/100 Base-T Connector Pinouts

Pin Number	Signal Name
1	Transmit positive
2	Transmit negative
3	Receive positive

Table A - 1: RJ-45 10/100 Base-T Connector Pinouts

Pin Number	Signal Name
4	Unused
5	Unused
6	Receive negative
7	Unused
8	Unused

Additional X506 Connectors

The X506 also supports a 1000 Base-T RJ-45 connector, as described in this section.

The following table describes the pinout information for the 1000 Base-T RJ-45 connector.

Table A - 2: RJ-45 1000 Base-T Connector Pinouts

Pin Number	Signal Name
1	Twisted Pair 1 positive (TP1+)
2	Twisted Pair 1 negative (TP1-)
3	Twisted Pair 2 positive (TP2+)
4	Twisted Pair 3 positive (TP3+)
5	Twisted Pair 3 negative (TP3-)
6	Twisted Pair 2 negative (TP2-)
7	Twisted Pair 4 positive (TP4+)
8	Twisted Pair 4 negative (TP4-)

Index

A

action set 17

C

chassis, X506 35
Class B digital apparatus 12
Command Line Interface (CLI) 18
configuration
 OBE Setup Wizard 27, 36
connecting to Internet 37
connecting X5 to Internet 28
connector & pinout specifications 39
content filtering 19
core functionality 18
customer support 9

D

DB-9 (COM) 39
Digital Vaccine 21

E

electrostatic discharge (ESD) 13, 15
encryption standards 19
environmental requirements 15
Ethernet interfaces 20

F

firewall 19

G

guide
 conventions 7
 organization 6
 overview 5
 related documentation 9
 target audience 5

H

hardware specifications
 X5 25
 X506 33

I

installation
 environmental requirements 15
 prepare the site 11
 safety requirements 12
 system grounding 15
 unpacking 16
installing chassis
 bolting device to rack 35
installing chassis,
 X506 35

installing X5 27
IPS core functionality 18
IPSec 19

L

L2TP 19
LEDs
 X5 24
 X506 32
Local Security Manager (LSM) 18, 21

M

management processor connectors
 DB-9 (COM) 39
 port connectors 39

P

power supply 27
PPTP 19
prepare the site 11
 environmental requirements 15
 safety requirements 12
 system grounding 15
 unpacking 16

R

rack space, X506 35
registering
 X5 28
 X506 37
related documentation 9
requirements
 environmental 15
 system grounding 15

S

Safety Extra-Low Voltage (SELV) 14
safety requirements 12
 ESD 13
Security Management System (SMS) 19,
 21, 26, 34
Security Zones 19
software specifications
 X5 26
 X506 34
Stateful IP filtering 17
system grounding requirements 15

T

tech support 9
Threat Management Center 9
Threat Management Center (TMC) 21
Threat Suppression Engine (TSE) 20
TMC 9
traffic performance 20

U

unpacking 16

V

VPN connectivity 19

X

X5 23
X506 31
X-Series core functionality 18